TRAITE COOPERATION EN MATIE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 29 juin 2000 (29.06.00)	
Demande internationale no PCT/FR99/02690	**Référence du dossier du déposant ou du mandataire** 76-0538
Date du dépôt international (jour/mois/année) 04 novembre 1999 (04.11.99)	**Date de priorité** (jour/mois/année) 17 novembre 1998 (17.11.98)
Déposant GUION, Christian	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

29 avril 2000 (29.04.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Antonia Muller

no de téléphone: (41-22) 338.83.38

Translation

09/856191

RECEIVED
MAR 27 2002
TECHNOLOGY CENTER 2800

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 76-0538	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR99/02690	International filing date (*day/month/year*) 04 November 1999 (04.11.99)	Priority date (*day/month/year*) 17 November 1998 (17.11.98)
International Patent Classification (IPC) or national classification and IPC G07F 7/10		
Applicant SCHLUMBERGER SYSTEMES		

RECEIVED
NOV 0 9 2001
Technology Center 2100

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 29 April 2000 (29.04.00)	Date of completion of this report 04 October 2000 (04.10.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR99/02690

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-8, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____.
pages _____, filed with the letter of _____.

☒ the claims, Nos. 1-12, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/3-3/3, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 99/02690

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-12	YES
	Claims		
Inventive step (IS)	Claims	1-12	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-12	YES
	Claims		NO

2. Citations and explanations

1. This report makes reference to the following document:

D1: US-A-5 550 919 (KOWALSKI JACEK) 27 August 1996 (1996-08-27)

2. Document D1 is considered the closest prior art and describes a device for limiting the number of attempts to intercept authentication operations.

The subject matter of independent Claim 1 differs from that disclosed in document D1 in that the device also includes an indicator element which can switch from a first state to a second state when the counter has reached the threshold value. The indicator element is separate from the counter element.

This solution does not follow obviously from the teaching of the documents cited in the International Search Report in combination with the knowledge of a person skilled in the art.

Consequently, the subject matter of independent Claim 1 satisfies the requirements of PCT Article

33(2, 3).

3. The requirement of industrial applicability is also satisfied (PCT Article 33(4)).

4. The subject matter of dependent Claims 2 to 12 also appears to satisfy the requirements of PCT Article 33.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Contrary to PCT Rule 5.1(a)(ii), the description does not indicate the relevant prior art disclosed in document D1 and does not cite that document.

16

T

TRAITE COOPERATION EN MATIE[redacted] DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 76-0538	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/02690	Date du dépot international *(jour/mois/année)* 04/11/1999	Date de priorité *(jour/mois/année)* 17/11/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G07F7/10		
Déposant SCHLUMBERGER SYSTEMES et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 4 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès d l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

I	☒	Base du rapport
II	☐	Priorité
III	☐	Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
IV	☐	Absence d'unité de l'invention
V	☒	Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
VI	☐	Certains documents cités
VII	☒	Irrégularités dans la demande internationale
VIII	☐	Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
29/04/2000	04. 10. 00
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Beauce, G N° de téléphone +49 89 2399 2519

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02690

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications.*) :

Description, pages:

1-8 version initiale

Revendications, N°:

1-12 version initiale

Dessins, feuilles:

1/3-3/3 version initiale

2. Les modifications ont entrainé l'annulation :

☐ de la description, pages :

☐ des revendications, n^{os} :

☐ des dessins, feuilles :

3. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

4. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications 1-12
	Non :	Revendications
Activité inventive	Oui :	Revendications 1-12
	Non :	Revendications
Possibilité d'application industrielle	Oui :	Revendications 1-12
	Non :	Revendications

2. Citations et explications

voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :

voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Il est fait référence au document suivant:
   D1: US-A-5 550 919 (KOWALSKI JACEK) 27 août 1996 (1996-08-27)

2. Le document D1 est considéré comme l'état de la technique le plus proche et décrit un dispositif permettant de limiter le nombre de tentatives d'interception des opérations de'authentification.

   L'objet de la revendication indépendante 1 diffère de celui divulgué dans le document D1 en ce que le dispositif comprend également un élément indicateur apte à passer d'un premier état à un second état lorsque le compteur a atteint la valeur seuil.L'élément indicateur étant distinct de l'élément compteur.

   Cette solution ne découle pas de façon évidente de l'enseignement transmis par les documents cités dans le rapport de recherche international en combinaison avec les connaissances de l'homme du métier.

   Par conséquent l'objet de la revendication indépendante 1 satisfait aux conditions de l'article 33(2,3) PCT.

3. La condition d'application industrielle est également satisfaite (Article 33(4) PCT).

4. L'objet des revendications dépendantes 2 à 12 semble également satisfaire aux conditions de l'article 33 PCT.

Concernant le point VII

Irrégularités dans la demande internationale

Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans le document D1 ne cite pas ce document.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 76-0538	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 99/ 02690	Date du dépôt international *(jour/mois/année)* 04/11/1999	(Date de priorité (la plus ancienne) *(jour/mois/année)* 17/11/1998
Déposant SCHLUMBERGER SYSTEMES et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

[X] le texte est approuvé tel qu'il a été remis par le déposant

[ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 2

[X] suggérée par le déposant.

[ ] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
[redacted]/FR 99/02690

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 5 550 919 A (KOWALSKI JACEK) 27 août 1996 (1996-08-27) abrégé colonne 1, ligne 10 colonne 2, ligne 48 - ligne 50 colonne 4, ligne 37 - ligne 49 revendications 1,6 ---	1-3,10, 12
X	US 4 879 645 A (TAMADA MASUO ET AL) 7 novembre 1989 (1989-11-07) abrégé colonne 1, ligne 35 - ligne 43 colonne 2, ligne 57 - ligne 68 revendications 1,4,6,9,12 --- -/--	1-3,10, 12

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 décembre 1999	22/12/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Wolles, B

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No [redacted]/FR 99/02690

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	FR 2 716 021 A (GEMPLUS CARD INT) 11 août 1995 (1995-08-11) abrégé page 1, ligne 1 - ligne 7 page 3 -page 6 revendications 1,3,4,6	1,2,5,6, 10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
[redacted]/FR 99/02690

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5550919 A	27-08-1996	FR 2705810 A	02-12-1994
		DE 69419967 D	16-09-1999
		DE 69419967 T	09-12-1999
		EP 0626662 A	30-11-1994
US 4879645 A	07-11-1989	JP 60207957 A	19-10-1985
		EP 0157303 A	09-10-1985
FR 2716021 A	11-08-1995	AT 156922 T	15-08-1997
		DE 69500561 D	18-09-1997
		DE 69500561 T	11-12-1997
		EP 0744063 A	27-11-1996
		ES 2105892 T	16-10-1997
		WO 9522125 A	17-08-1995
		US 5731576 A	24-03-1998

REPUBLIQUE FRANÇA[redacted]

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national
FA 567509
FR 9814409

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	US 5 550 919 A (KOWALSKI JACEK) 27 août 1996 (1996-08-27) * abrégé * * colonne 1, ligne 10 * * colonne 2, ligne 48 - ligne 50 * * colonne 4, ligne 37 - ligne 49 * * revendications 1,6 *	1-3,10, 12
X	US 4 879 645 A (TAMADA MASUO ET AL) 7 novembre 1989 (1989-11-07) * abrégé * * colonne 1, ligne 35 - ligne 43 * * colonne 2, ligne 57 - ligne 68 * * revendications 1,4,6,9,12 *	1-3,10, 12
A	FR 2 716 021 A (GEMPLUS CARD INT) 11 août 1995 (1995-08-11) * abrégé * * page 1, ligne 1 - ligne 7 * * page 3 - page 6 * * revendications 1,3,4,6 *	1,2,5,6, 10

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F

Date d'achèvement de la recherche	Examinateur
19 août 1999	Wolles, B

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

ANNEXE AU RAPPORT DE RECHERCHE PRELIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO.

FA 567509
FR 9814409

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

19-08-1999

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5550919 A	27-08-1996	FR 2705810 A	02-12-1994
		EP 0626662 A	30-11-1994
US 4879645 A	07-11-1989	JP 60207957 A	19-10-1985
		EP 0157303 A	09-10-1985
FR 2716021 A	11-08-1995	AT 156922 T	15-08-1997
		DE 69500561 D	18-09-1997
		DE 69500561 T	11-12-1997
		EP 0744063 A	27-11-1996
		ES 2105892 T	16-10-1997
		WO 9522125 A	17-08-1995
		US 5731576 A	24-03-1998

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G07F 7/10 — A1

(11) Numéro de publication internationale: WO 00/30047

(43) Date de publication internationale: 25 mai 2000 (25.05.00)

(21) Numéro de la demande internationale: PCT/FR99/02690

(22) Date de dépôt international: 4 novembre 1999 (04.11.99)

(30) Données relatives à la priorité:
98/14409 17 novembre 1998 (17.11.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: SCHLUMBERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F-92120 Montrouge (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: GUION, Christian [FR/FR]; 5, le Clos, F-91370 Verrières le Buisson (FR).

(74) Mandataire: UTZMANN-NORTH, Anne; Schlumberger Systèmes, Test & Transactions, 50, avenue Jean Jaurès, Boîte postale 620-12, F-92542 Montrouge Cedex (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

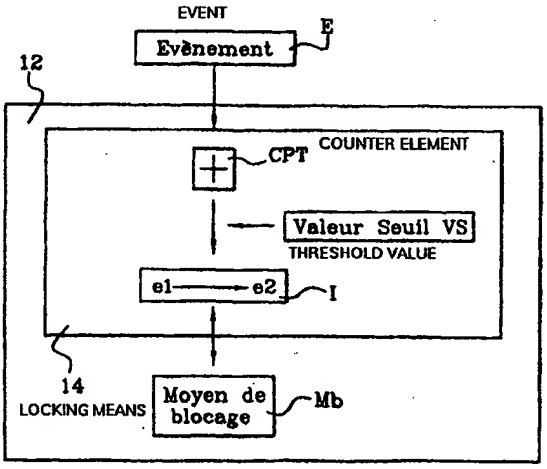
Publiée
Avec rapport de recherche internationale.

(54) Title: DEVICE FOR LIMITING FRAUD IN AN INTEGRATED CIRCUIT CARD

(54) Titre: DISPOSITIF POUR LA LIMITATION DE FRAUDES DANS UNE CARTE A CIRCUIT INTEGRE

(57) Abstract

The invention concerns an integrated circuit device containing a storage zone comprising a data storage unit. The invention is characterised in that said data storage unit comprises at least a counter element, at least an indicator element and at least a threshold value, said counter element counting at least the number of events having occurred in the device, and being capable of reaching said threshold value indicating a high maximum number of occurrences of said events, said indicator element being capable of passing from one first state to a second state when said counter element has reached said threshold value. The invention is applicable to smart cards.



(57) Abrégé

L'invention concerne un dispositif à circuit intégré contenant une zone mémoire comprenant une mémoire de données. L'invention se caractérise en ce que ladite mémoire de données contient au moins un élément compteur, au moins un élément indicateur et au moins une valeur seuil, ledit élément compteur comptant, d'une part, au moins un nombre d'occurrences d'événements survenus dans ledit dispositif, et, étant, d'autre part, susceptible d'atteindre ladite valeur seuil indicatrice d'un nombre maximum élevé d'occurrences desdits événements, ledit élément indicateur étant apte à passer d'un premier état à un second état lorsque ledit élément compteur a atteint ladite valeur seuil. L'invention s'applique, en particulier, aux cartes à puce.

DISPOSITIF POUR LA LIMITATION DE FRAUDES DANS UNE CARTE A CIRCUIT INTEGRE

La présente invention concerne un dispositif à circuit intégré contenant une zone mémoire comprenant une mémoire de données.

Un tel dispositif à circuit intégré est le plus souvent utilisé pour des applications dans lesquelles la sécurité du traitement d'informations est essentielle. Il s'agit en particulier de cartes à circuit intégré comportant des applications concernant le domaine de la santé, de la téléphonie mobile, ou encore, des applications relatives au domaine bancaire.

Une carte à circuit intégré se compose d'un corps de carte plastique dans lequel est incorporé un module électronique. Ladite carte communique avec un terminal, par exemple, un téléphone mobile, un terminal bancaire ou encore un ordinateur, via un réseau de communication et peut envoyer des messages contenant une information chiffrée audit terminal via ce réseau afin de sécuriser un transfert d'informations. Dans le langage courant, on dit que le message est signé. Pour le calcul de l'information chiffrée, la carte utilise une clef secrète de codage qui se trouve dans la mémoire de données de sa zone mémoire et un algorithme de cryptage.

Bien que le transfert d'informations soit ainsi sécurisé, une carte à circuit intégré reste vulnérable dans la mesure où un fraudeur peut effectuer un grand nombre d'actions sur la carte qui vont lui permettre de percer ses secrets. Ainsi, ledit fraudeur, désirant trouver ladite clef de codage, peut par exemple envoyer une instruction de signature d'un message à ladite carte et conserver la trace des signaux engendrés lors de l'exécution de ladite instruction. Par la suite, il peut envoyer un grand nombre d'instructions de signature du même message, soumettre la carte à des perturbations électromagnétiques à des instants précis du déroulement dudit algorithme et conserver les traces des différents

signaux émis. En établissant une correspondance entre les traces de signaux obtenues lors de perturbations et la première trace, ledit fraudeur peut étudier les différences ou l'absence de différences entre les diverses informations chiffrées obtenues pour découvrir une partie de la clef de codage. Ainsi, malgré le transfert d'informations sécurisées assuré par la carte, ledit fraudeur peut tout de même accéder à des informations confidentielles en effectuant un nombre très important d'actions sur la carte à circuit intégré.

Aussi, un problème technique à résoudre par l'objet de la présente invention est de proposer un dispositif à circuit intégré contenant une zone mémoire comprenant une mémoire de données, dispositif qui permettrait de mieux sécuriser la carte en limitant le nombre d'actions possibles sur la carte de la part d'un fraudeur.

Une solution au problème technique posé consiste, selon la présente invention, en ce que ladite mémoire de données contient au moins un élément compteur, au moins un élément indicateur et au moins une valeur seuil, ledit élément compteur comptant, d'une part, au moins un nombre d'occurrences d'événements survenus dans ledit dispositif, et, étant, d'autre part, susceptible d'atteindre ladite valeur seuil indicatrice d'un nombre maximum élevé d'occurrences desdits événements, ledit élément indicateur étant apte à passer d'un premier état à un second état lorsque ledit élément compteur a atteint ladite valeur seuil.

Ainsi, comme on le verra en détail plus loin, le dispositif de l'invention permet de limiter un nombre d'actions ou d'événements possibles sur ladite carte à circuit intégré grâce, d'une part, à un élément compteur qui comptera le nombre d'actions effectuées en prenant en compte une action ou un groupe d'actions, et, d'autre part, grâce à un élément indicateur qui indiquera qu'une valeur seuil d'occurrences d'événements ou d'actions a été atteinte ce qui permettra

par la suite de sanctionner un prochain dépassement de ladite valeur seuil.

La description qui va suivre au regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma d'un dispositif à circuit intégré selon l'invention, ici une carte à circuit intégré.

La figure 2 est un schéma représentant une zone mémoire de la carte de la figure 1 selon l'invention.

La figure 3 est un schéma montrant une répartition d'éléments compteurs et indicateurs dans la zone mémoire de la figure 2.

La figure 4 est un schéma montrant une autre répartition d'éléments compteurs et indicateurs dans la zone mémoire de la figure 2.

La figure 5 est un schéma d'une autre mise en oeuvre de l'invention, ladite zone mémoire de la figure 2 contenant deux éléments indicateurs identiques.

La figure 1 montre un dispositif 10 à circuit intégré, une carte à circuit intégré dans l'exemple de réalisation représenté.

Cette carte 10 contient un élément 11 de commande (par exemple une unité centrale de traitement ou CPU), une zone mémoire 12 contenant une mémoire 14 de données, et un bloc 13 de contacts destiné à une connexion électrique avec par exemple un connecteur d'un lecteur de cartes .

Ladite zone mémoire 12 est représentée sur la figure 2. Elle contient un élément compteur CPT, une valeur seuil VS, un élément indicateur I et un moyen Mb de blocage, ledit élément indicateur étant apte à passer d'un premier état e1 à un second état e2 lorsque ledit élément compteur a atteint ladite valeur seuil. Au cours de l'utilisation de ladite carte, plusieurs événements peuvent se produire, un

événement étant une action qui se produit dans ledit dispositif et qui aboutit à un résultat et dont on peut déterminer un nombre moyen d'occurrences dans l'utilisation dudit dispositif. Ainsi, par exemple, une mise sous tension est un événement qui aboutit à l'envoi par la carte d'un message, couramment appelé réponse au reset. L'envoi d'un message signé est également un événement.

Au cours de l'utilisation d'une carte, pour une application particulière, on peut déterminer un nombre moyen d'événements qui peuvent se produire, par exemple du type envoi de messages signés. Ainsi, pour une application bancaire, sur une période d'environ deux ans représentant la durée de vie d'une carte bancaire, il y aura en moyenne trois cent messages signés pour une carte appartenant à un utilisateur utilisant sa carte environ trois fois par semaine et six cent pour un utilisateur l'utilisant environ cinq fois par semaine.

Sur la figure 2, l'élément compteur CPT compte au moins un nombre d'occurrences d'événements survenus dans la carte, le nombre d'occurrences de messages signés par exemple. Ledit élément compteur est susceptible d'atteindre la valeur seuil VS indicatrice d'un nombre maximum élevé d'occurrences desdits événements. Dans le cas où la carte à circuit intégré comporte une mémoire non réinscriptible (ROM), une mémoire inscriptible (EPROM) et une réinscriptible (EEPROM), la valeur seuil VS, étant fixe, pourra se trouver dans l'une de ces trois mémoires, lesdites mémoires étant au sens du brevet une mémoire de données, tandis que les éléments compteurs et indicateurs se trouveront dans une mémoire réinscriptible, leur valeur étant variable.

Dans le cadre de l'invention, ladite valeur seuil représente un nombre improbable d'occurrences desdits événements se produisant dans ledit dispositif lors d'un usage normal dudit dispositif. De manière à déceler un usage frauduleux du dispositif, ledit nombre maximum d'occurrences d'événements est choisi élevé car il représente un nombre

improbable d'occurrences d'événements et ainsi, ledit nombre maximum élevé d'occurrences d'événements a une valeur supérieure à environ cent, préférentiellement supérieure à environ mille. Avec ces valeurs, on peut tenir compte de différents événements dans différentes applications. Dans l'exemple précité, on sait qu'il est improbable que deux mille occurrences de messages signés puissent se produire entre la carte et un terminal bancaire. Aussi, dans ce cas, la valeur seuil aura comme définition le nombre deux mille. Si un tel cas se produit, il est fort probable qu'un fraudeur essaye de percer les secrets de ladite carte.

Aussi, pour prévenir les fraudes, lorsque ledit élément CPT a atteint ladite valeur VS, ledit élément indicateur I passe d'un premier état e1 à un second état e2, on dit que l'élément I passe d'un état passif à un état actif et, de plus, le dispositif selon l'invention prévoit que ladite zone mémoire 12 comporte un moyen Mb de blocage du fonctionnement dudit dispositif lorsqu'un élément indicateur est passé dans le second état e2. Ainsi, si on atteint deux mille occurrences de messages signés, un élément I est activé et ledit moyen Mb de blocage, après avoir vérifié l'état dudit élément I, bloque ladite carte qui ne peut plus soit, recevoir ou produire aucun événement de même nature que celui qui a activé l'élément indicateur, ici un événement de type message signé, soit, recevoir aucun événement ni effectuer aucune action quelle qu'elle soit. Dans le dernier cas, ladite carte est inutilisable et on dit couramment que la carte est muette.

Suivant un premier mode de réalisation dudit dispositif selon l'invention, un élément compteur est défini pour un unique événement.

Ainsi, sur la figure 3, l'élément compteur CPT1 est défini pour l'événement E1, l'élément CPT2 pour l'événement E2 et l'élément CPT3 pour l'événement E3.

Cependant, bien que des événements puissent être de nature différente, leurs nombres d'occurrences dans la vie d'une carte peuvent

être du même ordre et par suite leurs nombres improbables d'occurrences peuvent être identiques. En conséquence, on peut vouloir les regrouper dans une même famille. Par exemple, on peut dire que l'envoi de messages signés fait partie de la même famille que l'envoi de messages cryptés. Aussi, suivant un deuxième mode de réalisation dudit dispositif selon l'invention, un élément compteur est défini pour au moins deux événements, lesdits événements faisant partie d'une même famille. Ainsi, selon le schéma de la figure 4, les éléments compteurs CPT1 et CPT2 sont définis respectivement pour les deux familles d'événements (E1, E2, E3) et (E4, E5).

Dans les deux modes de réalisation, l'invention prévoit qu'une valeur seuil est définie pour chaque élément compteur. Ainsi, cela revient à avoir, soit les valeurs VS1, VS2 et VS3 respectivement associées à chaque événement comme dans le cas de la figure 3, soit les valeurs VS1 et VS2 respectivement associées à chaque famille d'événements comme dans le cas de la figure 4. Lorsqu'un élément CPT a atteint sa valeur seuil VS, des éléments indicateurs indiquent que le nombre maximum d'occurrences d'événements autorisés représenté par la valeur seuil VS a été atteint.

Dans les deux modes de réalisation précités, il existe deux variantes de réalisation desdits éléments indicateurs.

Dans une première variante de réalisation montrée à la figure 3, le dispositif selon l'invention prévoit qu'au moins un élément indicateur I est défini pour un unique élément compteur CPT. Ainsi, lorsque l'élément compteur CPT1 atteint la valeur seuil VS1, l'élément indicateur I1 passe dans le second état e12. Le moyen Mb de blocage vérifie l'état dudit élément I1 et dès que celui-ci est passé dans le second état, il bloque ladite carte, il en est de même avec les éléments I2 et I3.

Dans une deuxième variante de réalisation montrée à la figure 4, le dispositif selon l'invention prévoit qu'au moins un élément indicateur I est défini pour au moins deux éléments compteurs CPT. Ainsi, lorsqu'un des éléments CPT1 ou CPT2 atteint respectivement sa valeur seuil VS1 ou VS2, l'élément I1 passe de l'état e11 à l'état e12 ce qui indique qu'une fraude a eu lieu et en conséquence, le moyen Mb bloque la carte.

Ainsi, suivant ces deux modes de réalisation et ces deux variantes de réalisation associées, on limite le nombre d'occurrences d'événements se produisant dans une carte et par suite le nombre d'actions possibles sur la carte de la part d'un fraudeur.

Cependant, un fraudeur pourrait modifier l'état d'un élément indicateur en le rendant passif s'il était actif auparavant, avant même que le moyen Mb n'ait pu bloquer ladite carte et par suite il pourrait en toute impunité continuer à percer les secrets de ladite carte.

Aussi, ladite mémoire 14 de données dudit dispositif selon l'invention contient au moins deux éléments indicateurs identiques se trouvant à des emplacements non contigus de ladite mémoire de données, lesdits éléments étant rattachés au même ensemble d'éléments compteurs contenant un ou plusieurs compteurs suivant les deux variantes précitées en relation avec les figures 3 et 4. Comme le montre la figure 5, l'élément indicateur I'1 est identique à I1 dans la mesure où ils sont tous deux rattachés aux éléments CPT1 et CPT2 et ils passent en même temps d'un premier état à un second état lorsque n'importe lequel de ces deux éléments compteurs a atteint sa valeur maximum. De plus, lesdits éléments indicateurs se trouvent dans la mémoire 14 de données de ladite carte à des endroits non contigus ce qui permet d'éviter une fraude qui consisterait à changer l'état de tous les éléments indicateurs identiques actifs, ladite fraude étant facilitée par le fait que les éléments seraient à des emplacements très proches

l'un de l'autre. Aussi, même si un fraudeur arrive à changer l'état d'un élément I en le rendant passif, les autres éléments indicateurs identiques resteront actifs car, dans ce cas, il sera improbable pour ledit fraudeur de trouver l'emplacement de tous les éléments indicateurs identiques.

Par ailleurs, le dispositif selon l'invention prévoit que ledit moyen Mb de blocage bloque le fonctionnement dudit dispositif lorsque l'état d'un élément indicateur est différent de l'état d'un autre élément indicateur identique. L'action du fraudeur est ainsi contrée.

On notera que dans tous les cas, les valeurs des premiers états des éléments indicateurs pourront être équivalentes ou différentes entre elles. Il en sera de même pour les valeurs des seconds états.

C'est ainsi que grâce aux deux modes de réalisation, aux deux variantes de réalisation des éléments indicateurs et ainsi qu'au système d'éléments indicateurs identiques, le dispositif selon l'invention permet de mieux sécuriser la carte en limitant le nombre d'actions possibles sur celle-ci de la part d'un fraudeur.

REVENDICATIONS

1 - Dispositif à circuit intégré contenant une zone mémoire comprenant une mémoire de données, caractérisé en ce que ladite mémoire de données contient au moins un élément compteur, au moins un élément indicateur et au moins une valeur seuil, ledit élément compteur comptant, d'une part, au moins un nombre d'occurrences d'événements survenus dans ledit dispositif, et, étant, d'autre part, susceptible d'atteindre ladite valeur seuil indicatrice d'un nombre maximum élevé d'occurrences desdits événements, ledit élément indicateur étant apte à passer d'un premier état à un second état lorsque ledit élément compteur a atteint ladite valeur seuil.

2 - Dispositif selon la revendication 1, caractérisé en ce qu'un événement est une action qui se produit dans ledit dispositif et qui aboutit à un résultat et dont on peut déterminer un nombre moyen d'occurrences dans la vie dudit dispositif.

3 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ladite valeur seuil représente un nombre improbable d'occurrences desdits événements se produisant dans ledit dispositif lors d'un usage normal dudit dispositif.

4 - Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'une valeur seuil est définie pour chaque élément compteur.

5 - Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'un élément compteur est défini pour un unique événement.

6 - Dispositif selon l'une des revendications 1 à 4, caractérisé en ce qu'un élément compteur est défini pour au moins deux événements.

7 - Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'au moins un élément indicateur est défini pour un unique élément compteur.

8 - Dispositif selon l'une des revendications 1 à 6, caractérisé en ce qu'au moins un élément indicateur est défini pour au moins deux éléments compteurs.

9 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ladite mémoire de données contient au moins deux éléments indicateurs identiques se trouvant à des emplacements non contigus de ladite mémoire de données.

10 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ladite zone mémoire comporte un moyen de blocage du fonctionnement dudit dispositif lorsqu'un élément indicateur est passé dans le second état.

11 - Dispositif selon les revendications 9 et 10, caractérisé en ce que ledit moyen de blocage bloque le fonctionnement dudit dispositif lorsque l'état d'un élément indicateur est différent de l'état d'un autre élément indicateur identique.

12 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ledit nombre maximum élevé d'occurrences d'événements a une valeur supérieure à environ cent, préférentiellement supérieure à environ mille.

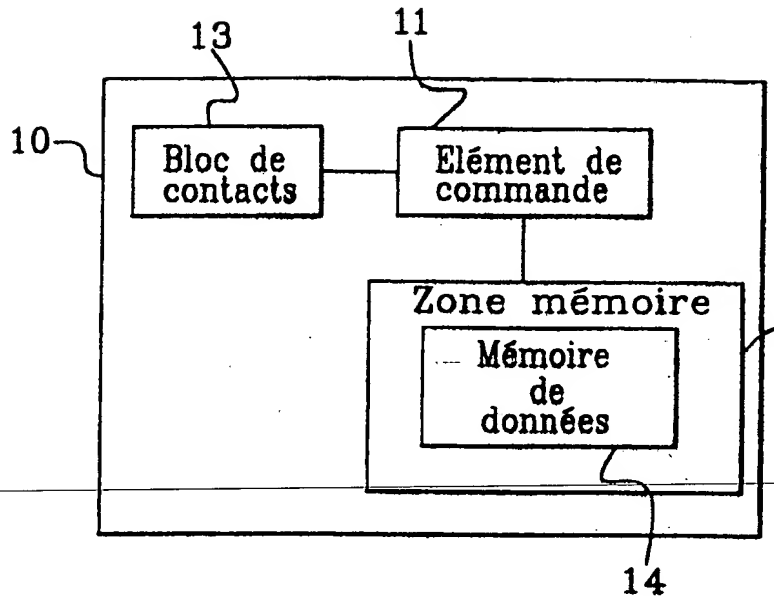

13
11
10
Bloc de contacts
Elément de commande
Zone mémoire
Mémoire de données
12
14

FIG.1

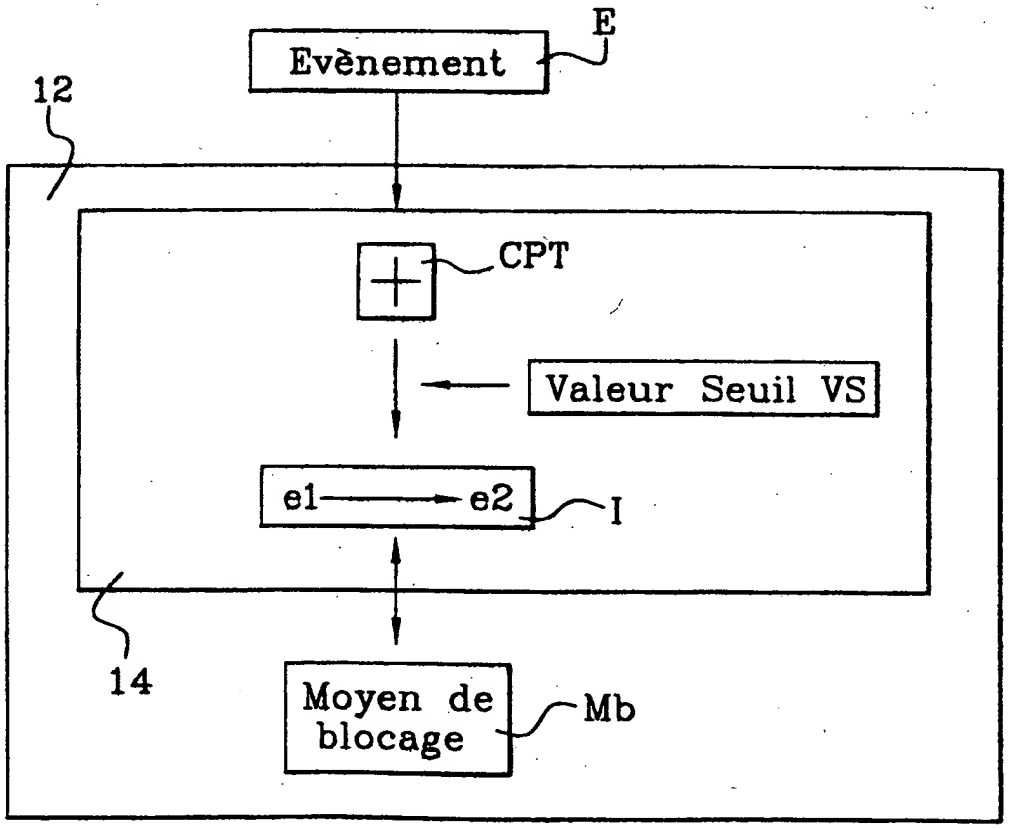
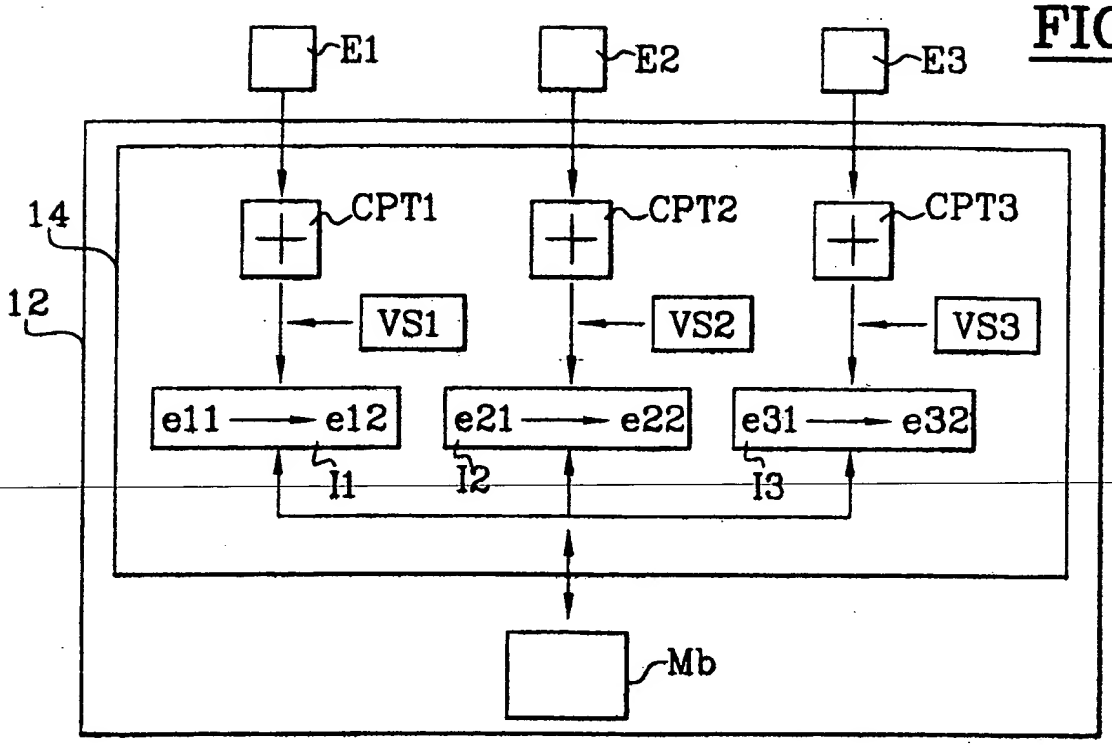

E
Evènement
12
CPT
Valeur Seuil VS
e1
e2
I
14
Moyen de blocage
Mb

FIG.2

FIG.3


E1
E2
E3
14
12
CPT1
CPT2
CPT3
VS1
VS2
VS3
e11
e12
e21
e22
e31
e32
I1
I2
I3
Mb

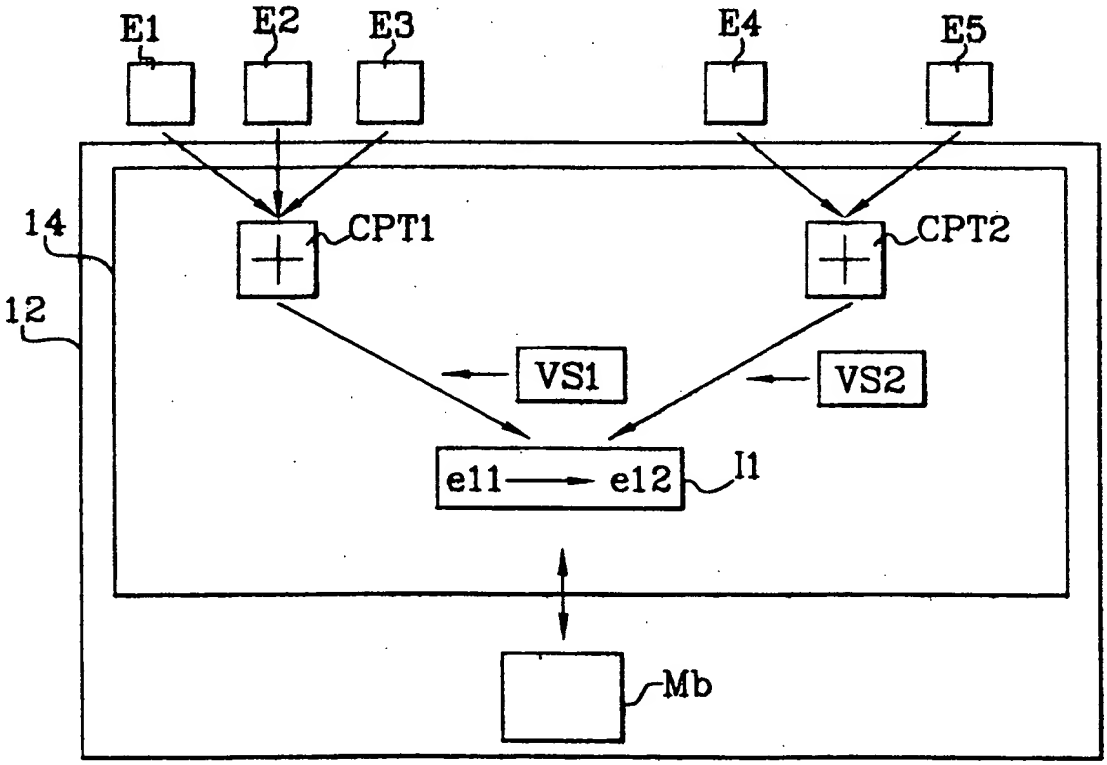

E1
E2
E3
E4
E5
14
12
CPT1
CPT2
VS1
VS2
e11
e12
I1
Mb

FIG.4

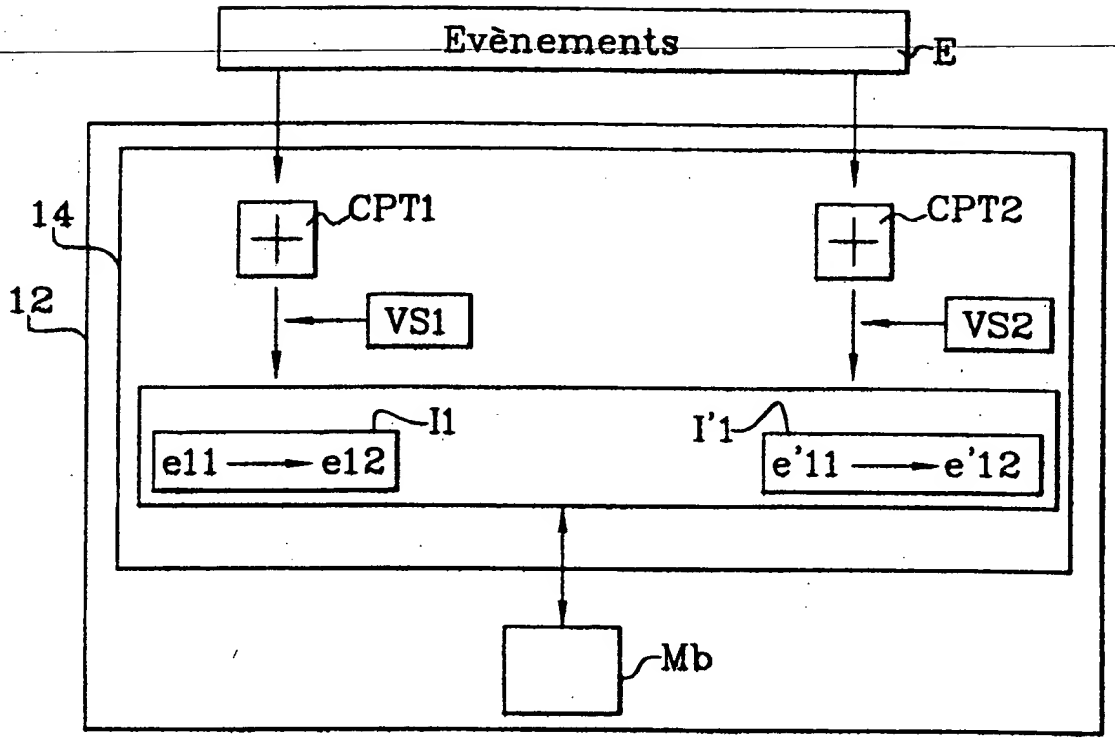


FIG.5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 99/02690

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 550 919 A (KOWALSKI JACEK) 27 August 1996 (1996-08-27) abstract column 1, line 10 column 2, line 48 - line 50 column 4, line 37 - line 49 claims 1,6 ---	1-3,10, 12
X	US 4 879 645 A (TAMADA MASUO ET AL) 7 November 1989 (1989-11-07) abstract column 1, line 35 - line 43 column 2, line 57 - line 68 claims 1,4,6,9,12 --- -/--	1-3,10, 12

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December 1999	22/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Wolles, B

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 99/02690

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 716 021 A (GEMPLUS CARD INT) 11 August 1995 (1995-08-11) abstract page 1, line 1 - line 7 page 3 -page 6 claims 1,3,4,6	1,2,5,6, 10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 99/02690

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5550919 A	27-08-1996	FR 2705810 A	02-12-1994
		DE 69419967 D	16-09-1999
		DE 69419967 T	09-12-1999
		EP 0626662 A	30-11-1994
US 4879645 A	07-11-1989	JP 60207957 A	19-10-1985
		EP 0157303 A	09-10-1985
FR 2716021 A	11-08-1995	AT 156922 T	15-08-1997
		DE 69500561 D	18-09-1997
		DE 69500561 T	11-12-1997
		EP 0744063 A	27-11-1996
		ES 2105892 T	16-10-1997
		WO 9522125 A	17-08-1995
		US 5731576 A	24-03-1998